June 11, 2018

Opening Remarks for the Colloquium for Information Systems Security Education
By
Dr. Vic Maconachy, Chairman of the Board.

Good Morning, and WELCOME.

The Colloquium is emerging as the professional organization for those dedicated to cybersecurity education. Our focus cannot be on the few schools who will eventually develop whole degree programs. We must look beyond that to all universities, to all 2- year schools, and yes, into the k-12 communities at large. A quick look tells me that in the USA there are 2,700 Universities 1,655 Community Colleges, and 37,100 High Schools. That does not bring into focus our potential partner schools outside of the USA. Our goal must be to transform the current state of cybersecurity education into programs, which integrate cybersecurity across all curricula. After all, how many ISC2 recognized professionals do not hold cybersecurity –specific degrees. How many professionals, without cybersecurity degrees, take those wonderful SANS courses? Those professionals are seeking to stay relevant in their fields. Isn't it time to get more proactive with our schools – at all levels, and across the globe?

We are so happy to see our partners from Great Britain here with us this week! They join with us in seeking global solutions for cybersecurity education.

The world needs cybersecurity degreed professionals, yes! The world also needs computer scientists, engineers, political scientist, educators, lawyers, business, financial, medical professionals, all prepared to enter their chosen careers, AND cybersecurity enabled. The NICE FRAMEWORK [1]speaks to this

A quick shout out to our partners from NIST who have joined with us this week!

But, achieving true integration into all curricula is no longer just a matter of political will. It is a matter of survival; survival requirements embraced – indeed – insisted upon by business and industry, not just the government. Cybersecurity is no longer

[1] https://www.nist.gov/.../nice-cybersecurity-workforce-framework

just a national security matter. Cybersecurity is now a national survival priority. The cyber threats represent a new, and perhaps more deadly set of weapons of mass destruction, including crippling cyber-kinetic capabilities. This is especially true when cyber is combined with other asymmetric attack weapons. Our national cyber defense forces are taught about this. Is it time to extend those learnings into the greater public cyber education domain.

What should be taught?

This past weekend, leaders from Purdue held a workshop to explore that very need. I hope we will hear of the results from those sessions from Spaf and Melissa. . As our nation, indeed the world enters into what some are calling, an era of hyperwar, we must rethink our academic content and directions. I urge you to review an article in the U. S. Naval Institute's Proceedings Magazine, "On Hyperwar", authored by retired U. S. Marine Corps General John R. Allen. This raises startling new questions on what we are now teaching our cybersecurity students.

This effort, to upgrade content is further complicated by the times in which we live. We used to think that the domain of Advanced Persistent Threats belonged solely with the government…UNTIL LAST WEEK! When the FBI provided a national announcement of a Russian cyber attack against routers. Including routers in businesses and homes. The case for the need for cybersecurity education at all levels could never be stronger.

Already we see signs of this emergence of need to reexamine what, indeed how, we prepare the current as well as future cybersecurity workforce. Just trying to understand the effects of Artificial Intelligence-related cybersecurity, and the introduction of quantum computing, exacerbates the urgency and depth of preparation needed.

In time, we will be offering support and assistance to those who desire to seek that integration into existing curricula. The debate, yes even the resistance to the inclusion of cybersecurity is the age-old question, "what has to go in order to make room for cybersecurity knowledge and skills in existing curricula?". Perhaps that is not the right question? The challenge falls to the accreditation bodies to step up to the needs of the 21st century. Some, under the leadership of visionaries such as Matt Bishop, Diana Burley, and Steve LaFountaine's team, have began to make those changes; changes brought about by the realization the cybersecurity knowledge and skills are no longer distinct from the essential skill sets for the modern day workers in the fields I mentioned, and many other fields. Those knowledge and skills sets

must now be taught, in and integrated fashion, with the knowledge and skills considered sacred to successful entry and participation in all career fields. As a former university administrator, I assure you the fastest way to achieve that integration is via the national accrediting bodies. Presidents and boards of trustees pay close attention to accreditations. Thank you ABET, ACM, and others for recognizing and acting on this national survival issue.

So, my fellow crusaders, I believe we have entered a new age of enlightenment. Along with that comes the realization that our fellow educators across our campuses need to be cultivated and supported into using and teaching essential cybersecurity knowledge and skills sets – integrated into their current programs of instruction. You should feel enabled to advocate the inclusion of cybersecurity topics across the curricula at your schools. Programs of instruction, being taught, not only in our colleges and universities, but also in our secondary schools. Many, like Davina Pruitt Mentle, of NIST, are also saying that practical and useful knowledge and skills in cybersecurity must also be introduced into the k – 12 curricula. Again, not in isolation, but via integration; integration which stresses cyber security as an essential life skill. Members of the Colloquium board are also devoting time and effort into this space. The timing for initiatives in this area could not be better, as the U. S. Dept. Of Education recently announced efforts to, "transform our k – 12 schools into places that use evidence-based practices to support social and emotional learning in parallel with academic learning." [2] Remember the Kennedy-era requirements for physical fitness programs? In this age of cybersecurity enlightenment, Strong – safe minds and bodies must now also include cyber hygienics! We have no trouble teaching safe sex, we should have no problem teaching safe hex.

How will we achieve this in America, indeed on a global scale?

Membership in an organization dedicated to that mission and focus, is a great step forward. A goal many of us have been working towards for many years. It is time that the role of cybersecurity educator stands tall next to already recognized professions in this field. Later, in this Colloquium, we will discuss how we all can band together, as members in this emerging field, to seek necessary change and resources to better enable us in our missions. In short, the world is turning to us to become the bastions of defense, producing students now and for the future who will preserve and protect critical cyber systems and capabilities.

---

[2] Washington Post. May 27, 2018. Melania Trump's Good Idea. By Timothy Shriver. p A19.

So, welcome to Colloquium 22. Now for a Colloquium tradition. Those of you attending for the first time, please stand. For the rest of us who have participated before, please reach out and welcome our new members. Thank you all, so much for all that you do.

God Speed!